THE CLAIMS

A complete listing of all of originally filed Claims 1 – 36 is provided below. A status identifier is provided for each claim in a parenthetical expression following each claim number.

1.   (Currently Amended) A proxy method comprising:

receiving encrypted data from a client over an unsecure network ~~in a first hop~~;

decrypting the encrypted data into decrypted data;

~~performing a test relative to~~ examining the decrypted data~~, the test yielding one of at least a first result and a second result; and,~~ for security purposes;

re-encrypting the examined decrypted data; and

~~in response to the test yielding the first result, sending the decrypted data~~ sending the re-encrypted data to an origin server over a given network~~ in a second hop~~.

2.   Canceled

3.   Canceled

4.   (Currently Amended) The proxy method of claim 1, wherein the given network is a secure network.

5.   (Currently Amended) The proxy method of claim 4, wherein the ~~decrypted data is sent to the origin server over the given network in the second hop~~ sending is in accordance with one of the hypertext transport protocol (HTTP), the post office protocol (POP), the wireless access protocol (WAP), ~~and~~ or the Internet messaging access protocol (IMAP).

6.   (Currently Amended) The proxy method of claim 1, wherein the given network is one of the unsecure network and a second unsecure network.

7.   (Currently Amended) The <u>proxy</u> method of claim 1, wherein the ~~encrypted data is received from the client over the unsecure network in the first hop~~ <u>receiving is</u> within a secure socket layer (SSL) session.

8.   (Currently Amended) The <u>proxy</u> method of claim 1, wherein the unsecure network is the Internet.

9.   (Currently Amended) The <u>proxy</u> method of claim 1, wherein the origin server is an effective origin server.

10.   (Currently Amended) The <u>proxy</u> method of claim 1, wherein the client is an effective client.

11.   (Currently Amended) The <u>proxy</u> method of claim 1, wherein the method is performed by a proxy within the given network.

12.   (Currently Amended) The <u>proxy</u> method of claim 1, wherein the method is performed by a firewall within the given network.

13.   (Currently Amended) A computer-readable medium having a computer program stored thereon for execution by a processor to perform the <u>proxy</u> method of claim 1.

14.   (Currently Amended) A <u>proxy</u> method comprising:
receiving unencrypted data from a client over a secure network ~~in a first hop~~;
~~performing a test relative to~~ <u>examining</u> the unencrypted data~~, the test yielding one of at least a first result and a second result~~ <u>for security purposes</u>; and,

in response to the ~~test~~ examining yielding that the ~~first result,~~ unencrypted data does not present a security risk:

encrypting the unencrypted data into encrypted data;

sending the encrypted data to an origin server over an unsecure network ~~in a second hop~~.

15.   Canceled

16.   (Currently Amended) The proxy method of claim 14, wherein the unencrypted data is received from the client over the secure network ~~in the first hop~~ in accordance with one of the post office protocol (POP), the Internet messaging access protocol (IMAP), the hypertext transport protocol (HTTP), ~~and~~ or the wireless access protocol (WAP).

17.   (Currently Amended) The proxy method of claim 14, wherein the ~~encrypted data is sent to the origin server over the unsecure network in the second hop~~ sending is within a secure socket layer (SSL) session.

18.   (Currently Amended) The proxy method of claim 14, wherein the secure network is a carrier network.

19.   (Currently Amended) The proxy method of claim 14, wherein the unsecure network is the Internet.

20.   (Currently Amended) The proxy method of claim 14, wherein the client is a thin client.

21.   (Currently Amended) The <u>proxy</u> method of claim 14, wherein the client is
one of a: personal digital assistant (PDA) device, a laptop computer, a notebook computer,
~~and~~ <u>or</u> a wireless phone.

22.   (Currently Amended) The <u>proxy</u> method of claim 14, wherein the secure
network is one of a wireless network ~~and~~ <u>or</u> a wired network.

23.   (Currently Amended) The <u>proxy</u> method of claim 14, wherein the client is an
effective client.

24.   (Currently Amended) The <u>proxy</u> method of claim 14, wherein the origin
server is an effective origin server.

25.   (Currently Amended) The <u>proxy</u> method of claim 14, wherein the method is
performed by a proxy within the secure network.

26.   (Currently Amended) The <u>proxy</u> method of claim 14, wherein the method is
performed by a firewall within the secure network.

27.   (Currently Amended) A computer-readable medium having a computer
program stored thereon for execution by a processor to perform the method <u>proxy</u> of claim
14.

28.   (Currently Amended) A system comprising:
a client to send encrypted data over an unsecure network ~~in a first hop~~;
a proxy within a secure network to receive the encrypted data<u>,</u> ~~and~~ decrypt the
encrypted data into decrypted data, ~~the proxy sending~~ <u>perform a test relative to the
decrypted data, and send</u> the decrypted data over the secure network ~~in a second hop~~ <u>in</u>

response to ~~performing a~~ the test ~~relative to the decrypted data~~ yielding a particular response; and,

an origin server within the secure network to receive the decrypted data.

29.   (Currently Amended) The system of claim 28, wherein the client is an effective client comprising:

a second client within a second secure network to send unencrypted data over the second secure network ~~in an additional hop~~; and,

a second proxy within the second secure network to receive the unencrypted data, ~~the second proxy encrypting~~ encrypt the unencrypted data into the encrypted data, perform a second test relative to the unencrypted data, and ~~sending~~ send the encrypted data over the unsecure network ~~in the first hop~~ in response to ~~performing a~~ the second test ~~relative to the unencrypted data~~ yielding a second particular response.

30.   (Currently Amended) The system of claim 28, wherein the client is an effective client comprising:

a second client to send second encrypted data over the unsecure network in an additional hop; and,

a second proxy to receive the second encrypted data, ~~and~~ decrypt the second encrypted data into second decrypted data, ~~the second proxy encrypting~~ perform a second test relative to the second decrypted data, encrypt the second decrypted data into the encrypted data, and ~~sending~~ send the encrypted data over the unsecure network ~~in the first hop~~ in response ~~to performing a~~ the second test ~~relative to the unencrypted data~~ yielding a second particular response.

31.   (Currently Amended) A system comprising:

a client to send unencrypted data over a secure network ~~in a first hop~~;

a proxy within the secure network to receive the unencrypted data, ~~the proxy~~ perform a test relative to the unencrypted data, ~~encrypting~~ encrypt the unencrypted data

into encrypted data~~,~~ and ~~sending~~ <u>send</u> the encrypted data over an unsecure network ~~in a second hop~~ in response to ~~performing a~~ <u>the</u> test ~~relative to the unencrypted data~~ yielding a particular response; and,

an origin server to receive the encrypted data.

32.   (Currently Amended) The system of claim 31, where the origin server is an effective origin server comprising:

a second proxy within a second secure network to receive the encrypted data~~,~~ ~~and~~ decrypt the encrypted data into decrypted data, ~~the second proxy sending~~ <u>and send</u> the decrypted data over the second secure network ~~in an additional hop~~; and,

a second origin server within the second secure network to receive the decrypted data.

33.   (Currently Amended) A proxy comprising:

one or more communication components enabling the proxy to communicate over a first network and a second network;

a processor; and,

a computer-readable medium having a computer program stored thereon for execution by the processor to<u>:</u>

receive data that is originally encrypted or unencrypted from a client over the first network ~~in a first hop and~~<u>:</u>

decrypt the data where the data was originally encrypted,

perform a test relative to the data~~,~~ <u>~~yielding one of at least a first result and a second result, and~~</u>

in response to the test yielding ~~the first~~ <u>a particular</u> result, ~~sending~~ <u>send</u> the data unencrypted to an origin server over the second network ~~in a second hop~~ where the data was originally encrypted, ~~and sending~~ <u>or send</u> the data unencrypted or encrypted to the origin server over the second network ~~in a second hop~~ where the data was originally unencrypted.

34.   (Original)   The proxy of claim 33, wherein the first network is a secure network.

35.   (Currently Amended) The proxy of claim 33, wherein the second network is an unsecure network, such that sending the data to the origin server over the second network ~~in the second hop~~ comprises first encrypting the data.

36.   (Original)   The proxy of claim 33, wherein the second network is a secure network.